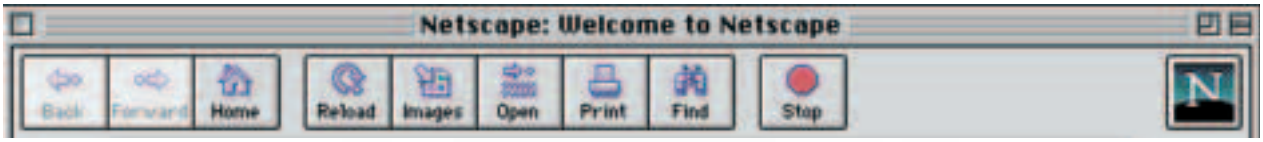

Internet

Böse, böse Cyberwelt!

Macht die Luken dicht! (II)

Viele von uns können sich ein Leben – sei es beruflich oder privat – ohne Internet schon fast nicht mehr vorstellen. Aber, wie verschiedene Vorkommnisse der letzten Zeit deutlich gemacht haben (Lovsan, Sobig.F und seine potentiellen Nachfolger ...), werden die Zeiten und die Sitten immer rauer auf dem uns so lieb gewordenen Web. Die Techniken der Hacker und anderer unliebsamer Geister aus der Gilde der Programmierer werden zunehmend raffinierter und perfider. Seinen PC gegen Angriffe von aussen abzuschotten, dient nicht mehr nur dem Schutz vertraulicher Daten und Transaktionen, sondern hilft auch, sich viel Ärger (und manchmal auch Geld) zu ersparen. Wie eine Litanei weisen Experten immer wieder darauf hin, dass ein einigermassen effizienter Schutz nur mit einem regelmässig upgedateten Anti-Viren-Programm und einer Firewall zu erzielen ist. In der letzen Rubrik wurden die Prinzipien dieser Brandschutzmauern vorgestellt. Diesmal stelle ich Ihnen zwei für die private Nutzung kostenlose Programme vor, die gegen die meisten Attacken einen guten Schutz gegen Angriffe aus dem Internet bieten. Gegenüber teureren Alternativen muss der Anwender höchstens einige Abstriche beim Funktionsumfang und den Konfigurationsmöglichkeiten machen.

Thomas Vauthier
Th.vauthier@bluewin.ch

ZoneAlarm: kostenloser Klassiker

ZoneAlarm unterscheidet zwischen Internet und Ihrer lokalen Zone, beispielsweise dem Netzwerk in Ihrer Praxis oder zu Hause. Es gilt allgemein, dass Sie gegenüber dem Internet höchste Sicherheit walten lassen sollten, in der lokalen Zone genügt der mittlere Level.

Zonen definieren: Im Reiter «Security» enthält der Button «Advanced» eine Liste mit allen wichtigen Netzwerk-Verbindungen; hier können Sie jene markieren, die zur lokalen Zone gehören. Einzelne Rechner oder vertrauenswürdige Bereiche können mit «Add» hinzugefügt werden.

«Splashscreen» abschalten: So surfen Sie ohne Störung. Wenn die Alarme Sie stören (mit denen ZoneAlarm nicht geizt), desaktivieren Sie in «Alerts» einfach «Show the Alert Pop-up Windows».

Bestimmen, welches Programm ins Web darf: ZoneAlarm fragt Sie für jedes Programm per Popup, ob es auf das Internet zugreifen darf. Benutzen Sie in der ersten Lernphase alle Internetprogramme, die Sie in Zukunft nutzen wollen, damit Sie diesen den Zugang ins Internet erlauben können. ZoneAlarm sollte Sie dann im täglichen Gebrauch nur noch selten stören. Taucht trotzdem eine Warnung auf, hat sie meist wirklich etwas zu bedeuten.

Klicken Sie hierzu auf «Programs», um die Liste der Anwendungen zu bearbeiten. In der Spalte «Allow connect» können Sie sowohl für Ihr lokales Netz als auch für den Internetzugang bestimmen, welches Programm eine Onlineverbindung benötigt. Ihrem E-Mail-Programm und dem FTP-Client können Sie alle Zugriffe erlauben, für Hilfsprogramme wie dem Windows Media Player bietet sich maximal die Abfrage an – vielleicht wollen diese Multimediaprogramme nur Abspiel-Codes nachladen.

Server-Dienste sperren und freigeben: In der selben Liste bestimmen Sie auch, welche Programme als Server fungieren können – nur ist «Server» in ZoneAlarm ein eigener Begriff. Gemeint sind hier Programme, die im Laufe einer Internetkommunikation aktiv Daten erwarten und entgegennehmen. Anwendungen wie FTP-Tools, Mail-Clients oder der Real Player benötigen für die ordnungsgemässen Funktion Server-Rechte. Gleiches gilt für Filesharing-Systeme, Messenger und Chat-Clients.

Allerdings reissen diese Server-Rechte Lücken in Ihre Firewall: Die entsprechenden Ports sind offen und für Scanner sichtbar, solange die Anwendung läuft. Gehen Sie deshalb sparsam mit diesen Rechten um, und beenden Sie die Programme, sobald diese ihren Job erledigt haben. In kritischen Fällen können Sie unter «Security» über die Option «Block Internet Server» Programme sofort sperren, denen Sie Server-Rechte zugestanden haben.

Outpost: die individuelle Firewall

Outpost ist eine kostenlose Toplösung für erfahrene Anwender: Mit leicht verständlichen Regeln können Sie das Online-Verhalten Ihrer Programme genau anpassen, Ihren E-Mail-Client sichern und dabei einige Viren blocken.

Im Selbstlernmodus bietet Ihnen Outpost an, zu Anwendungen gleich Regeln zu erstellen. Nutzen Sie die Presets, die im Rolldown-Menü von Outpost zu finden sind. Das Programm richtet dann automatisch Regeln für Softwarekategorien wie Browser, Mail-Programme, FTP- und Chat-Clients ein.

Individuelles Feintuning: Damit eher problematische Programme keine Zugriffsrechte bekommen, sollten Sie die Regeln regelmässig prüfen. Den Regel-Editor finden Sie unter «Option | Anwendungen». Um eine Regel hinzuzufügen, müssen Sie die Anwendung allerdings zunächst einem der drei Bereiche «Blockierte», «Eingeschränkt Erlaubte» und «Vertraute Anwendungen» zuordnen.

Auto-Blocker aktivieren: Outpost besitzt eine Funktion zum automatischen Blockieren eines Angreifers, versteckt diese allerdings in «Optionen | Plugin-Setup». Dort finden Sie auch andere Plug-ins, welche die Funktionalität von Outpost modular aufwerten. Klicken Sie auf «Attack Detection» und «Eigenschaften» und aktivieren Sie die Checkbox «Blockiere IP des Angreifers für ...». Wenn Sie den Benachrichtigungslevel auf «Hoch» stellen, schlägt Outpost Alarm, sobald ein Angreifer Sie auf Sicherheitslücken scannt.

Weitere Plug-ins konfigurieren: Über die Eigenschaften von «Active Content Filter» können Sie jeweils für den Internet Explorer und Ihr E-Mail-Programm das Ausführen von ActiveX und anderen verdächtigen Web-Technologien verhindern. Schalten Sie die Optionen für »E-Mail, News« so um, dass alle Einstellungen desaktiviert sind – damit schützen Sie Outlook vor ActiveX-Viren oder JavaScript-Popups.

Fortsetzung fogt ...